RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: CLS-M06

The Journey of Enterprise Network Micro-Segmentation at Scale

Todd Outten

Distinguished Engineer
Comcast Cyber Security

LinkedIn

Jeff Stoklosa

Principal Cyber Security Engineer
Comcast Cyber Security

LinkedIn

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

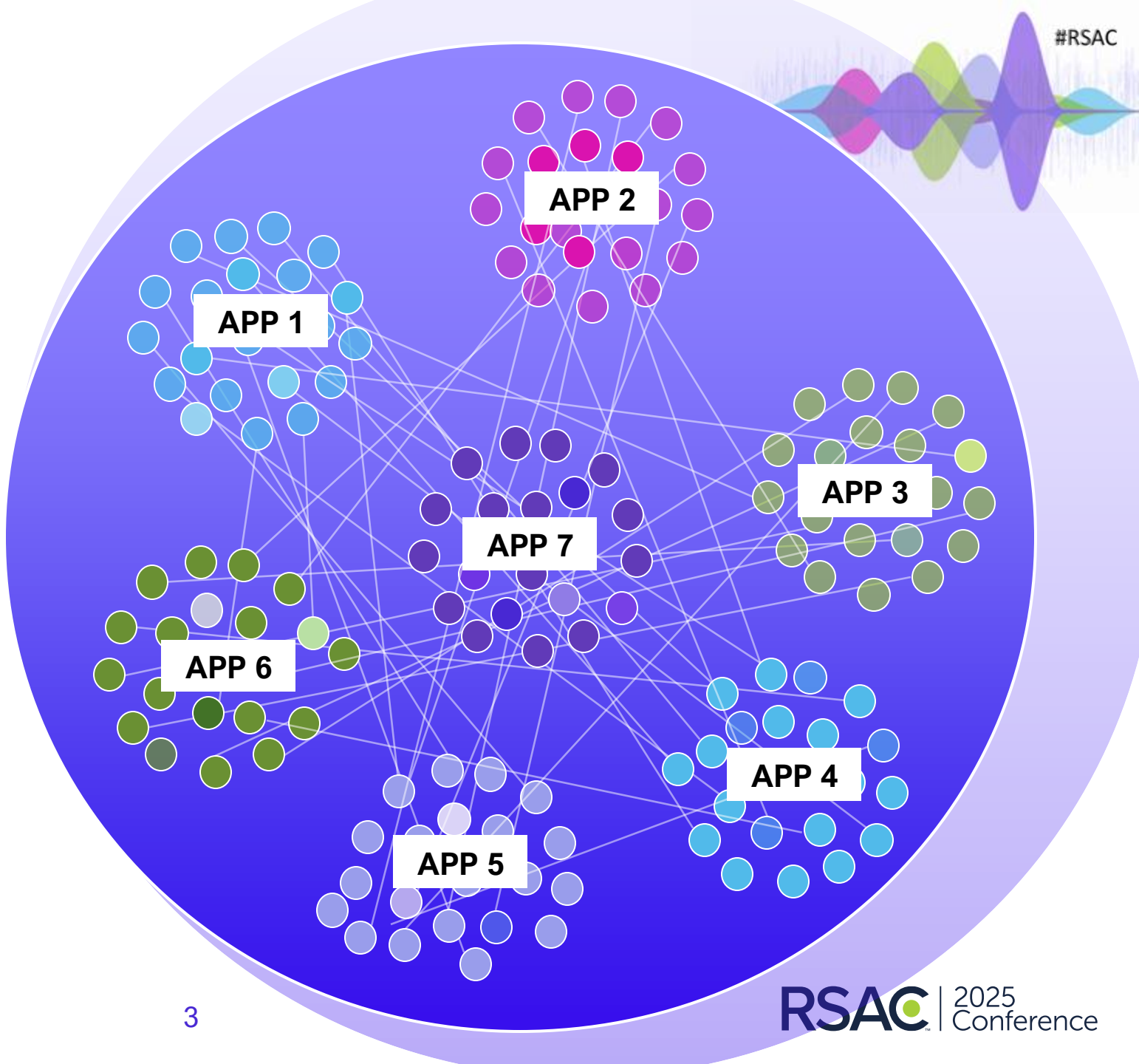
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

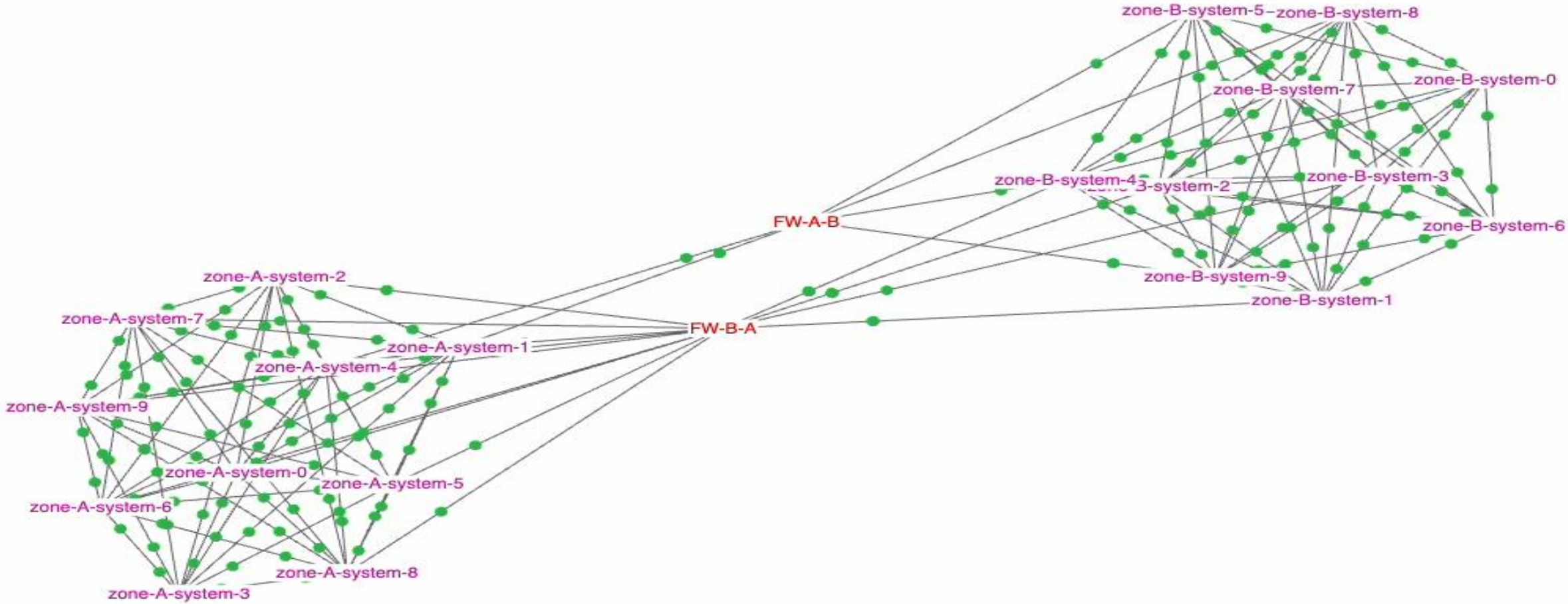
Problem Statement

If a system was compromised in your environment, how easily could the threat actor move from one system to the next?

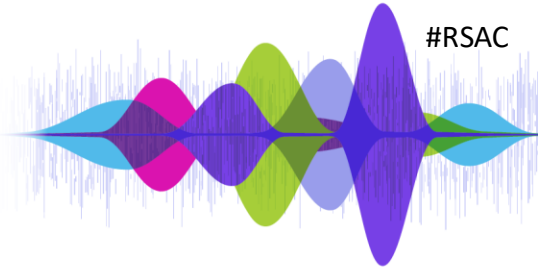
- Is your attack surface larger than it needs to be?
- Are key systems at risk if another system is compromised?
- Do you have a lack of visibility?
- Can you find proper ownership?
- Are Firewall Rules overprovisioned with lots of implicit access?



Problem Statement



Zero Trust Network Micro-Segmentation



That is where we were … Now we are headed *here* …

Key items we needed to solve:

- Reduce attack surfaces
- Declarative and Transparent Access Policies
- Clear Ownership of Applications, Services, and Communication
- Data Driven Decisions
- Ability to audit each Application and identify recommendations for Best Practices and Access Policy Hygiene

Tenant Security Framework

TSF increases Comcast's security posture while providing a user-friendly network micro-segmentation solution for our engineers.

NIST (National Institute of Standards and Technology)

- Zero Trust Architecture
- Policy Decision Point
- Policy Enforcement Point

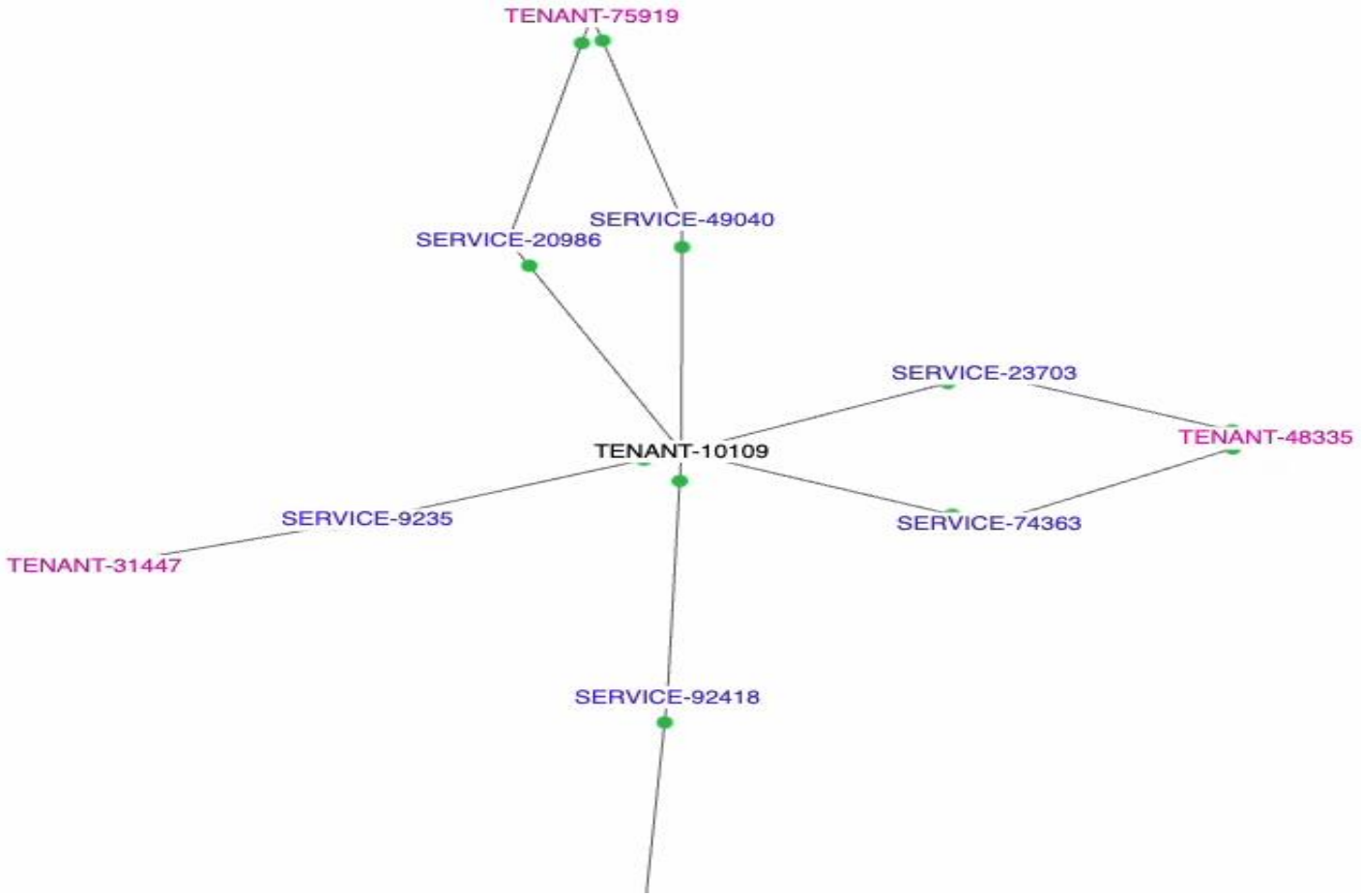
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Tenant Security Framework (**TSF**): Comcast's approach to Zero Trust Network Micro-Segmentation.

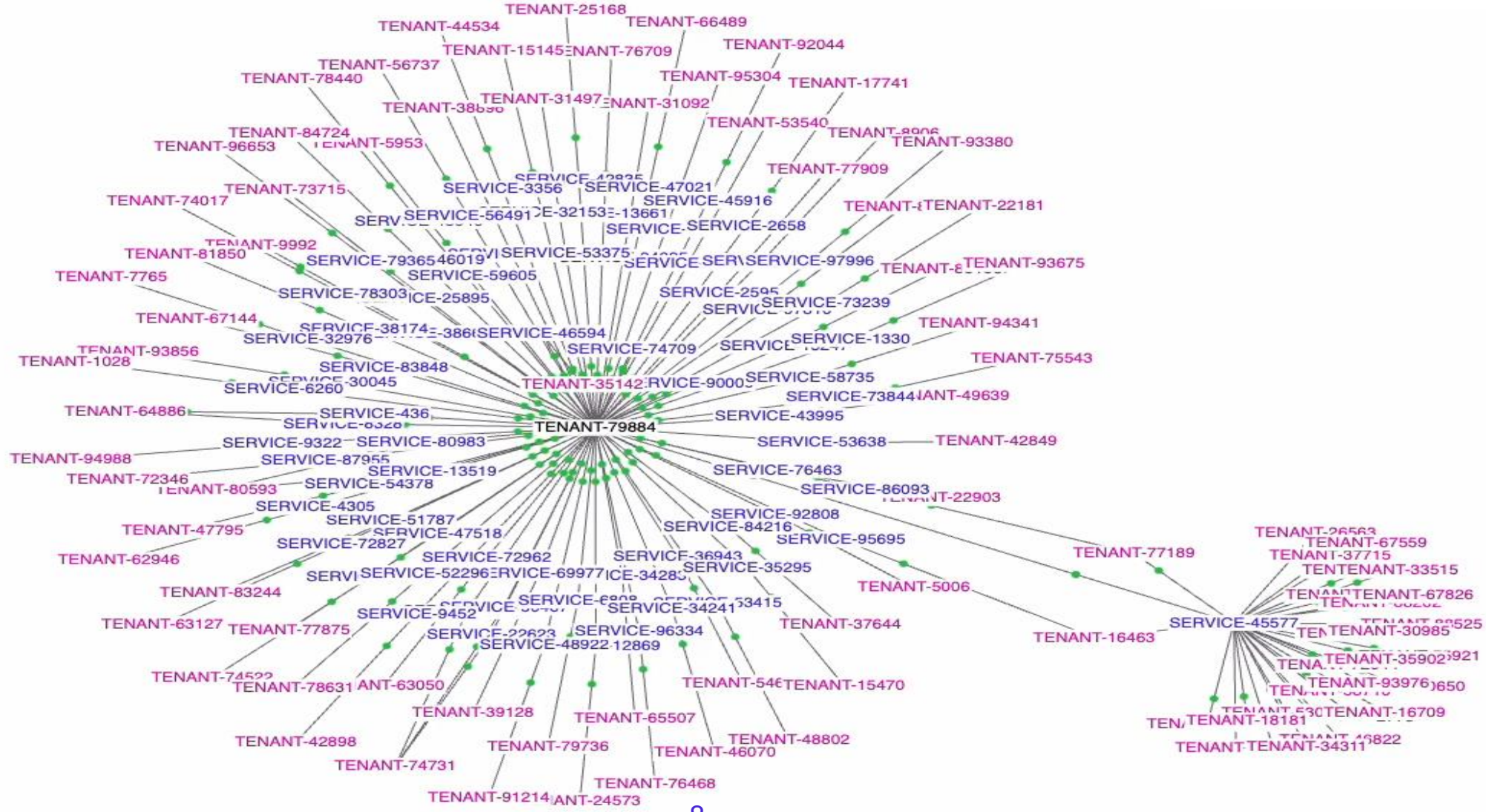
Tenant: A container for an application and its components, infrastructure, networks, services, and access policies. The fundamental concept of the TSF Framework.

Access Policy: Declarative statement from a Source Tenant to a Specific Service in a Destination Tenant.

Goals: Typical Tenant



Goals: Enterprise Services



RSAC 2025 Conference

Keys to Success

Keys to Success for Micro-Segmentation

MULTI-CLOUD & HYBRID

SUPPORTS MULTIPLE PLATFORMS SO CUSTOMERS CAN RUN THEIR WORKLOADS IN THE BEST ENVIRONMENT

AUTOMATION & SELF-SERVICE

USES AUTOMATION TO QUICKLY AND CONSISTENTLY DEPLOY AT SCALE

LEADERSHIP

CROSS ORGANIZATION ALIGNMENT

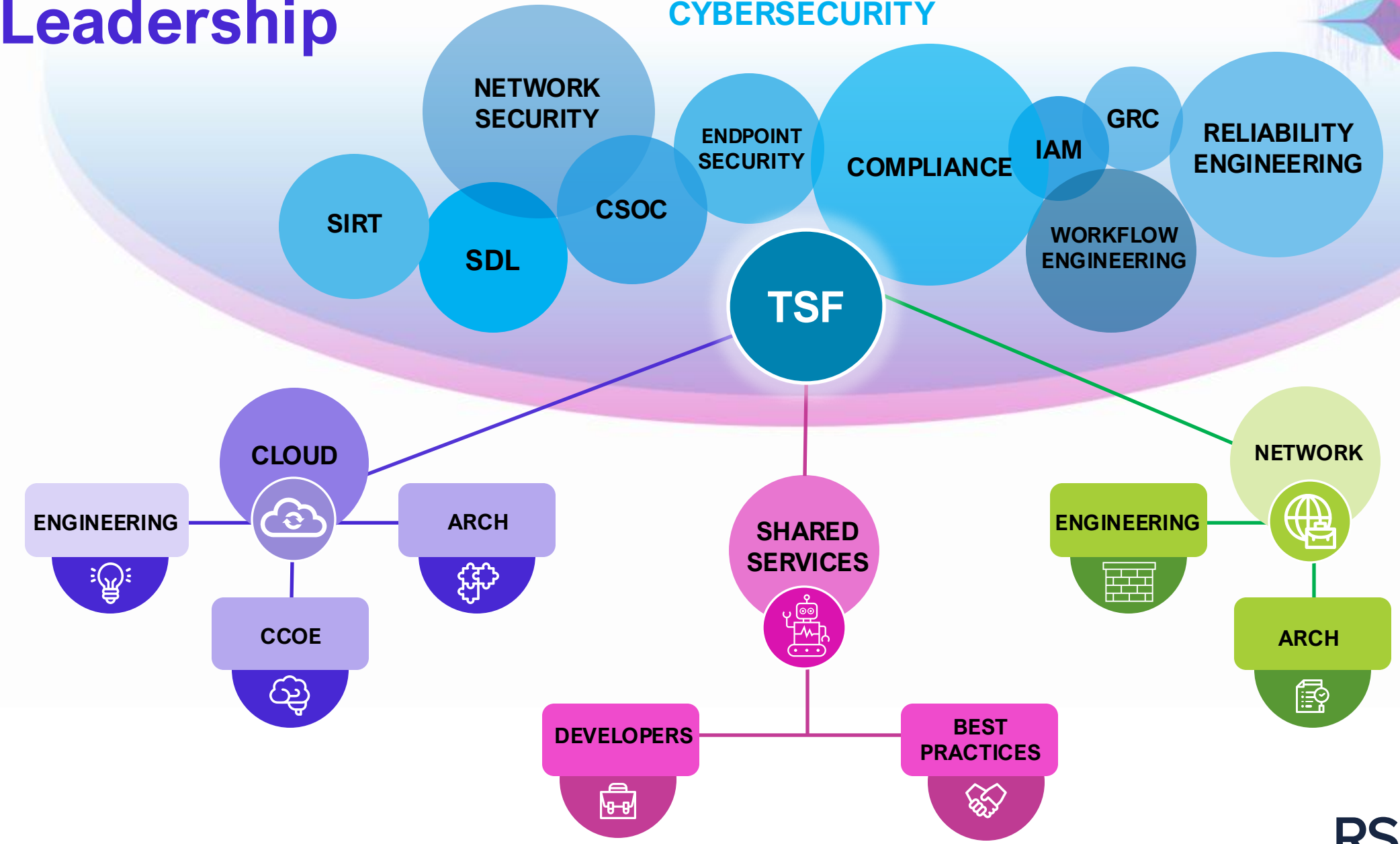
DATA (VISIBILITY)

CLOUD GOVERNANCE PROVIDES A CLEAR VIEW OF WORKFLOW STATUS AND CONFIGURATION

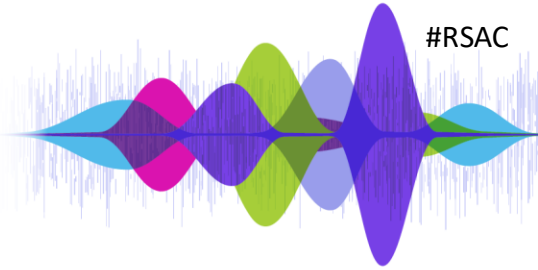
FRAMEWORK

DESIGNED TO ADAPT TO BOTH CLOUD AND NON-CLOUD ENVIRONMENTS

Leadership


CYBERSECURITY
NETWORK SECURITY
ENDPOINT SECURITY
COMPLIANCE
IAM
GRC
RELIABILITY ENGINEERING
SIRT
SDL
CSOC
WORKFLOW ENGINEERING
TSF
CLOUD
ENGINEERING
ARCH
CCOE
SHARED SERVICES
DEVELOPERS
BEST PRACTICES
NETWORK
ENGINEERING
ARCH

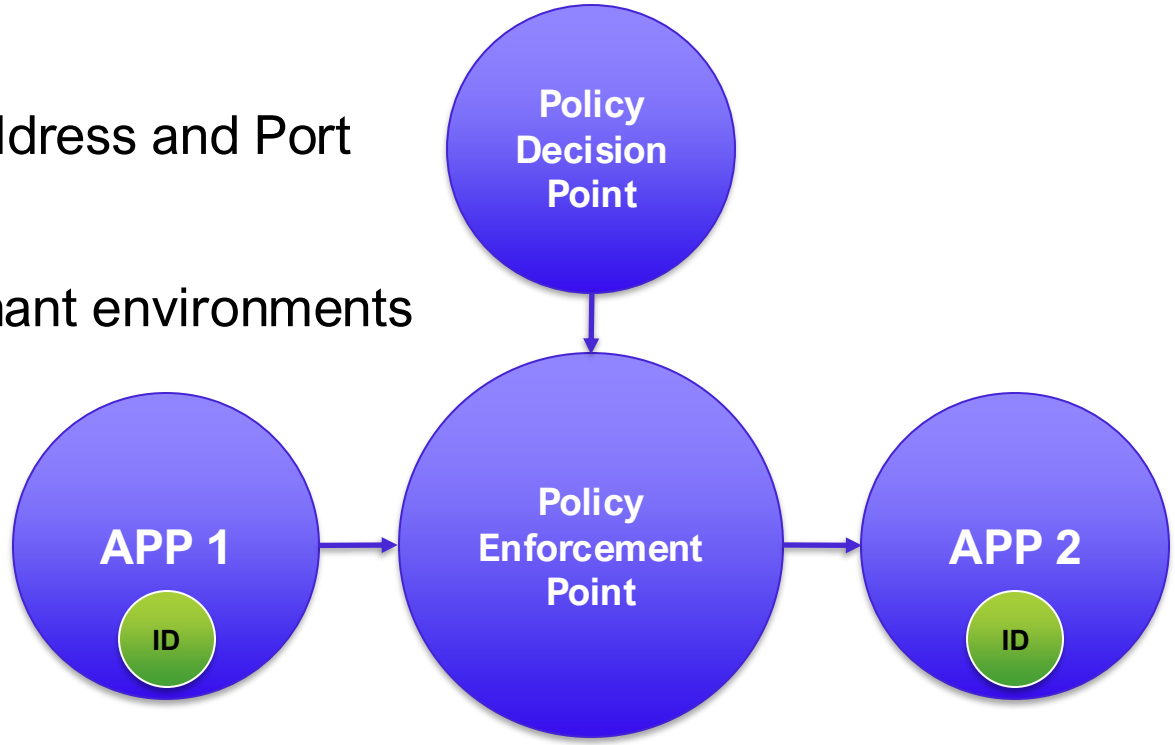
The Framework



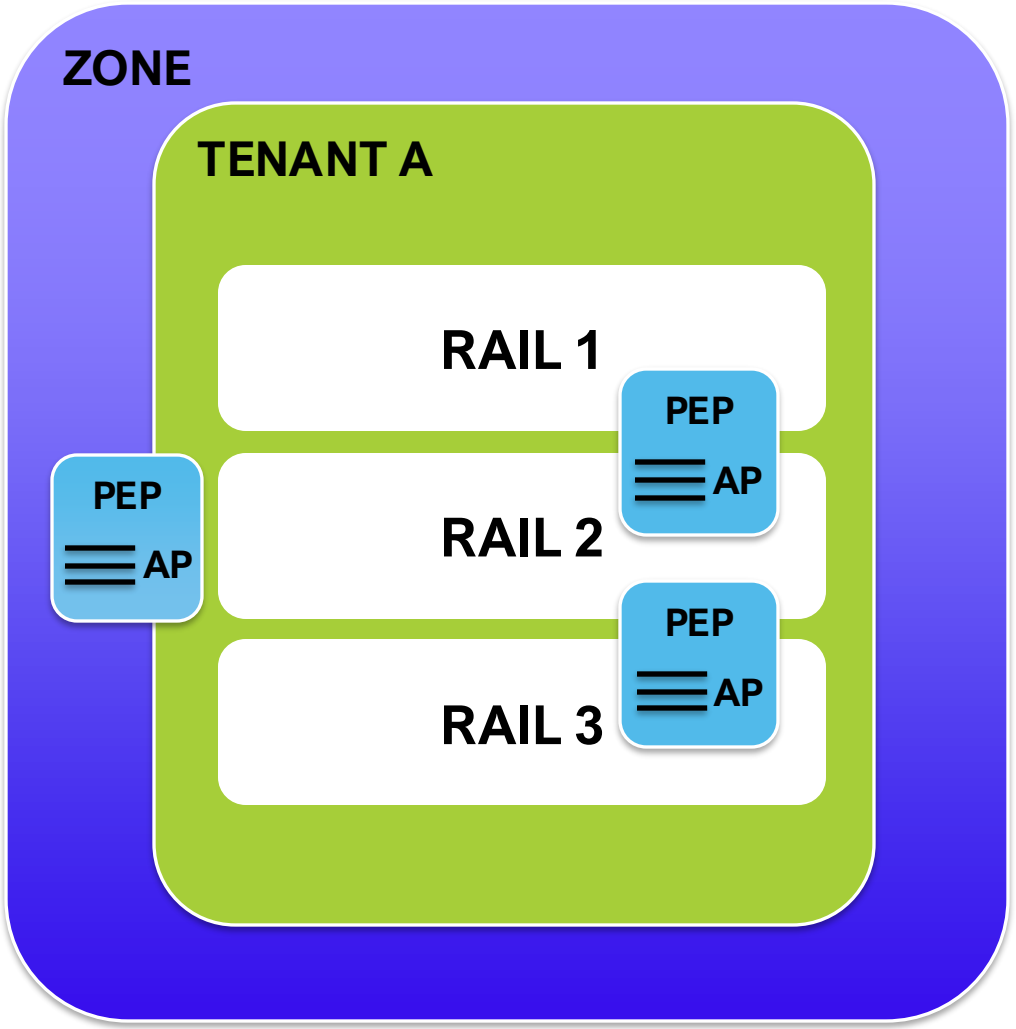
- **You do not need to do this alone**
  - There is Industry Guidance to research
    - NIST Zero Trust Architecture
- We suggest a framework that is flexible and can be used across your environment(s)
- Cybersecurity and platform teams are responsible for managing PEPs and PDPs
- Application Owner's are responsible for the management, configuration, and maintenance of their Tenant

Thinking about the Framework

- **Tenant Identity**
  - Solution needed to address multi-cloud and hybrid
    - TCP/IP Layer 3 and 4
      - Lowest Common Denominator – IP Address and Port
    - Creates the boundary for segmentation
    - Expands to other ID methods in multi-tenant environments
- **Policy Enforcement Point**
  - Enforces the access policy or rules
  - Must be in every environment
- **Policy Decision Point**
  - Structuring the data and decisions



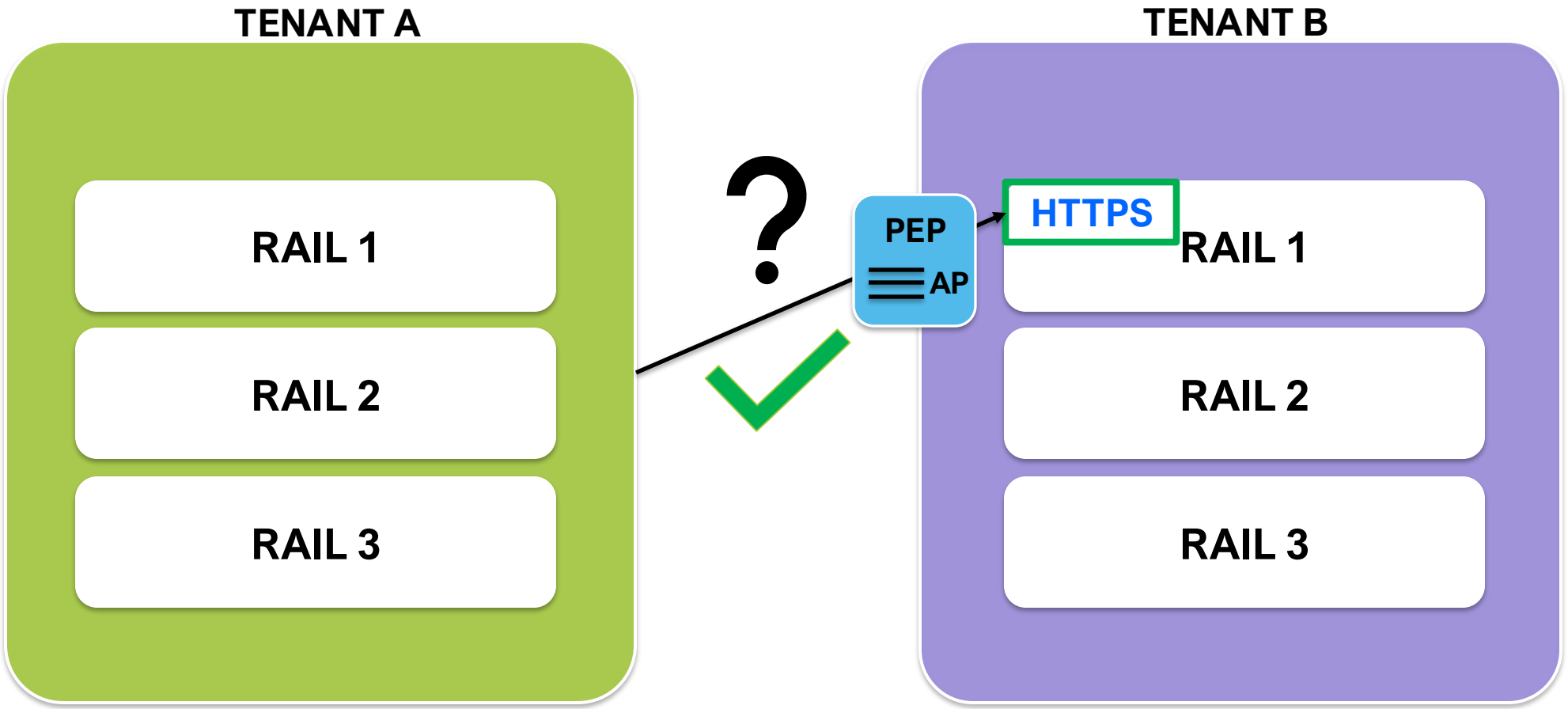
Framework Key Components



- A "**Zone**" comprises of many like tenants
- A Tenant is comprised of an application stack deployed onto rails
- Tenants begin life with Zero Trust
- A rail comprises like systems of an application
- Policy Enforcement Points (**PEP**) contain declarative Access Policies (**AP**)

#RSAC
RSAC 2025 Conference

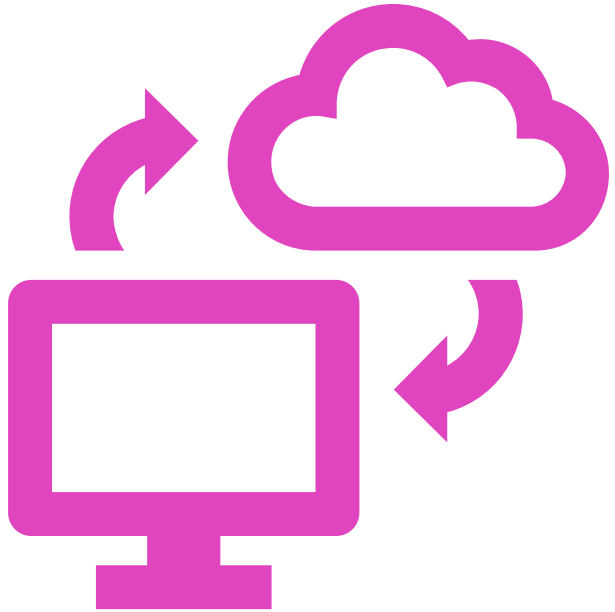
The Framework



Data (Visibility)

- **Data structure**
  - Creating a series of registries that are platform agnostic
    - Allows for the Framework to expand to new technologies
- **Helps eliminate the black box for application owners**
    - Models the relationships between workloads
- **Identify Best Practices & Anti-Patterns**
- **Data Driven Decisions**

Multi-Cloud & Hybrid

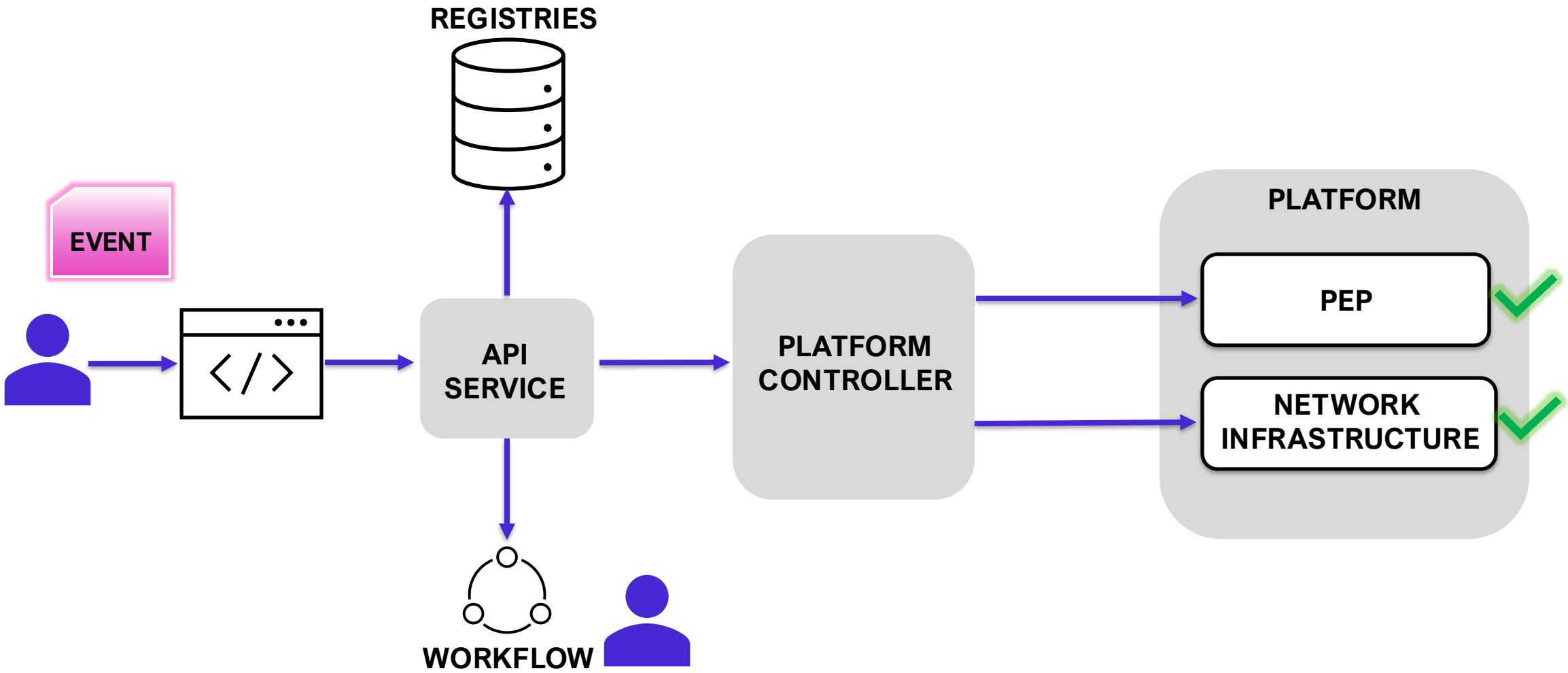


- **Addressing multiple platforms**
  - Take advantage of using native controls of platform
    - Private Clouds
    - Bare Metal
    - Public clouds
    - Kubernetes
- **Understand how the framework can be enabled on each platform**
  - You probably have all the tools you need
- **Reduce friction with developers letting them focus on their strengths**
  - Single, comprehensive UI
  - Challenge - developers needed to support subnets and access policies where they did not need to think about that previously

Automation and Self-Service

- **Automation is key!**
  - Increases velocity
  - Greater standardization
  - A single source to be able to provision infrastructure and access policies
- **Workflow management**
  - Can implement any flows or approvals needed
  - Automated approvals
- **Developed software layer** (Controller)
  - Renders implementation on native platform controls

Walkthrough of an example event

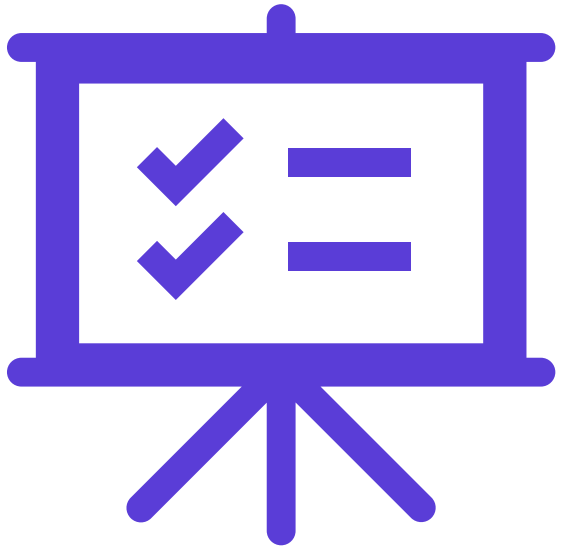


RSAC 2025 Conference

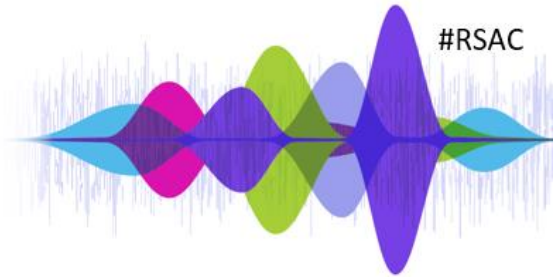
Past, Present and Future

Results: What have we seen

- **Efficacy**
  - Analysis revealed, there is **a lower rate of** Endpoint Detection & Response for known malicious patterns & behaviors for TSF hosts compared to non-TSF endpoints.
  - Most applications do not require broad access to services
    - The median number of user defined access policies is 6 ingress and 6 egress
- **Teams want their Applications to be secure at scale**
- **Velocity for changes**



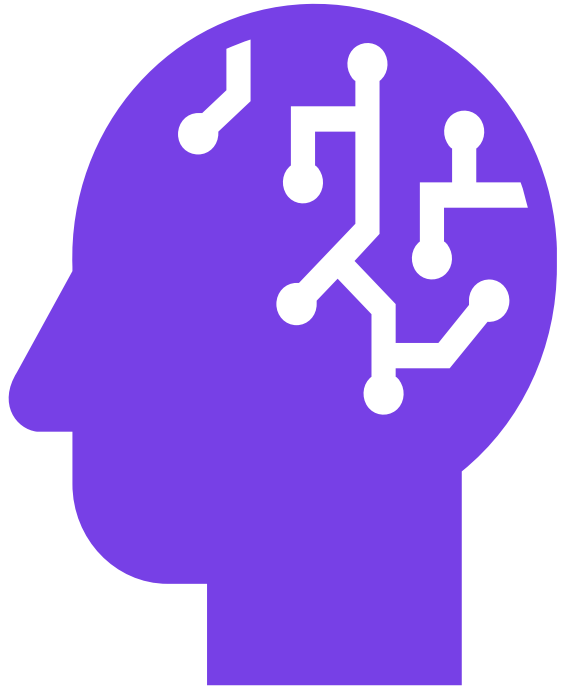
Lessons Learned



- **Micro-Segmentation is doable at scale**
  - *Native controls of each platform*
  - *Cap and grow – find a suitable environment*
    - *Crawl, Walk, Run & Iterate*
- **Customer Experience**
  - Secure Development Lifecycle requires good data
- **Applications Developers are not Network Engineers**
  - Answer: good documentation, training, tooling, self service
  - Provide tools to help Application Owners discover their connectivity requirements
- **Incremental improvements to make our security better**
  - Be Agile … don't take on everything at once
- **Customer migrations**
  - Greenfield provides better opportunities for starting
  - Harder to retrofit existing environments
- **Use data to audit and measure efficacy**
- **Think thoroughly about Internet Ingress and Egress**
  - Done through approvals and justification

The Future

- **More Platforms**
  - “Layer 7” for dynamic, cloud native platform
  - Increasing the speed of platform enablement via code reuse, common observability, and tools development
- **Auditing**
  - Real-time NetFlow analysis of Access Policies
  - Best Practices and ability to give Tenant Owners recommendations for most secure configuration
- **Dynamic Policies**
  - Once a year, quarter, month, day
- **More micro, and more micro**
- **Cross-Organizational Collaboration**
  - Standards and Open Source



RSAC 2025 Conference

Apply

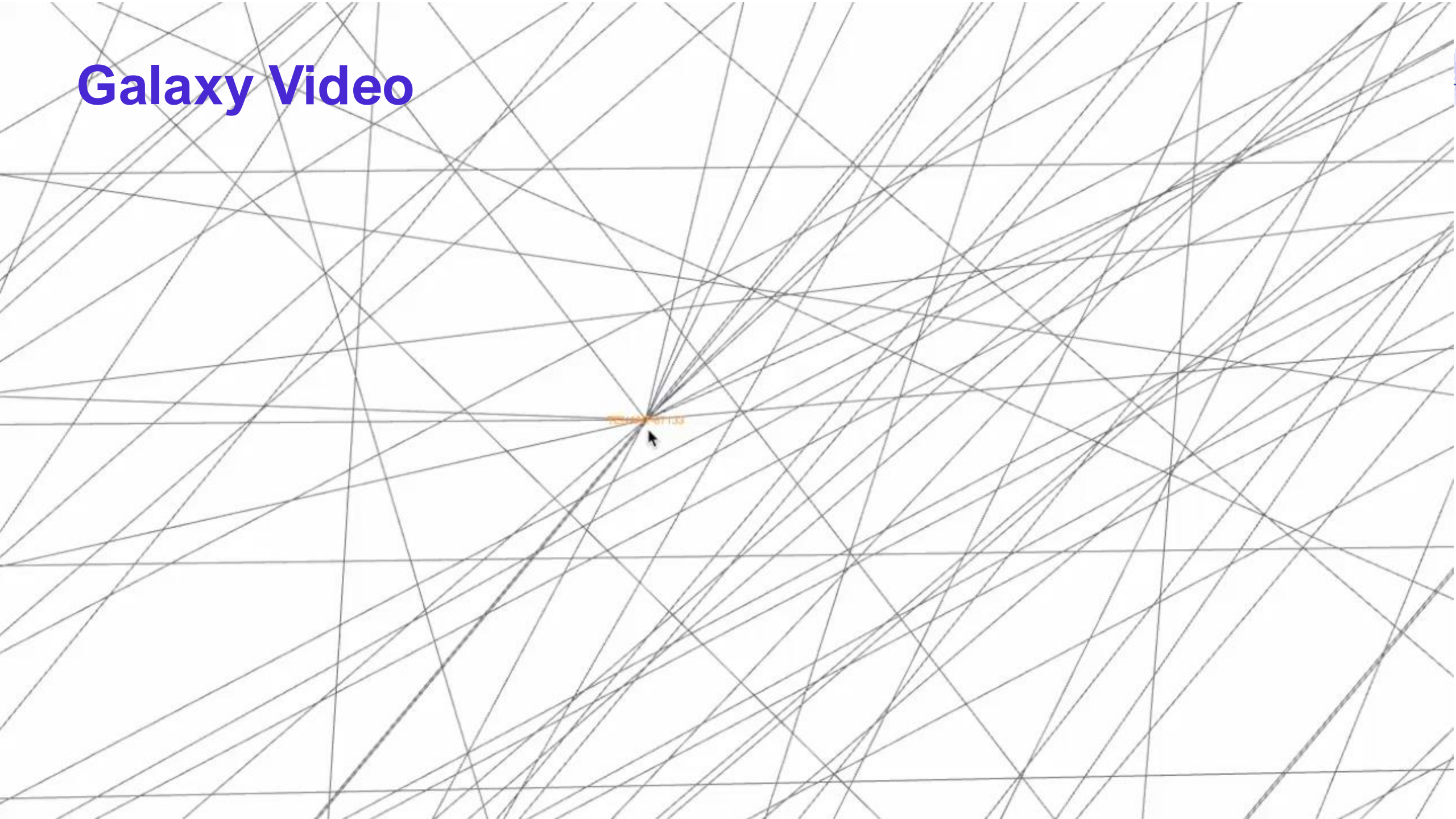
Homework

- **Understand your current ecosystem**

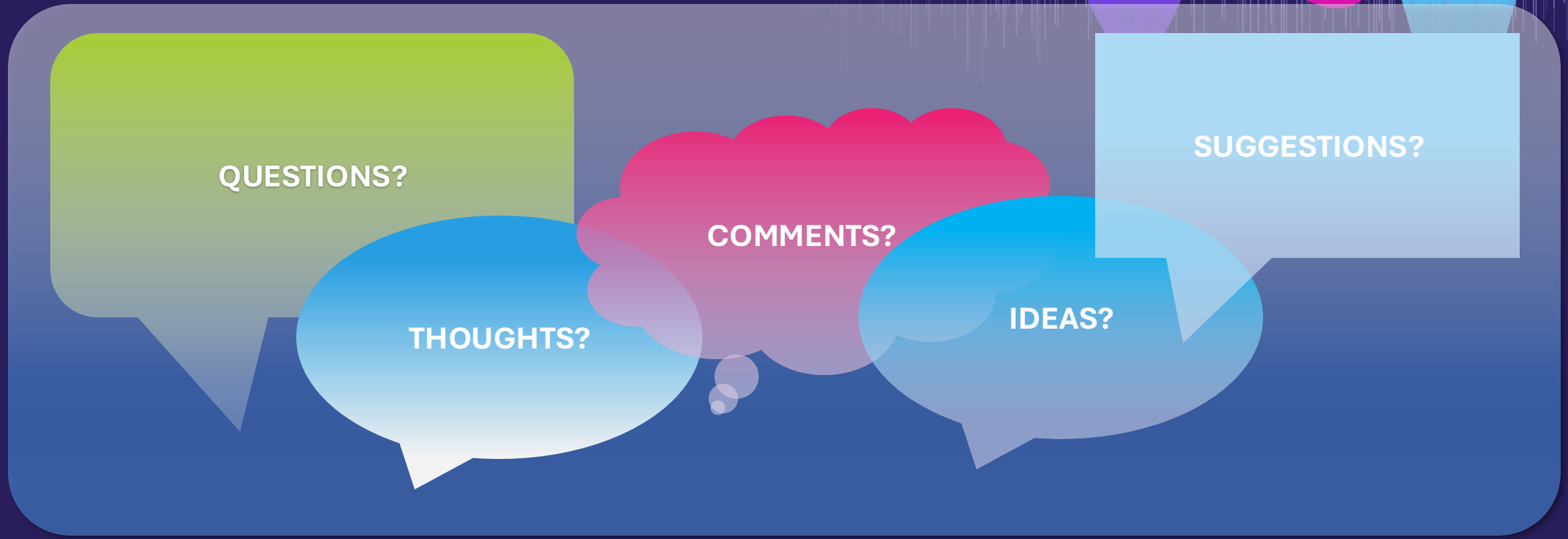
- **Begin to Develop a framework**
  - **Start Small**: Pick one platform or even one internal application
    - What policy enforcement points exist for the application and platform?
    - Is the application physically or virtually segmented from other applications?
    - How can workloads be identified across the network?

- **Longer term:**
  - Determine how to measure the Efficacy of your Network Micro-Segmentation Initiatives
  - *Get involved with Industry Standards and Approaches*

Galaxy Video



RSAC 2025 Conference

Many Voices.
One Community.

Thank You